

ADVANCED PROJECTS

Protect your identity online

Internet shoppers, political dissidents and sufferers of embarrassing ailments can all benefit from anonymity on the net. Jon Thompson explains how the Tor network can help

Why would anyone want to use the internet anonymously? While the innocent may think they have nothing to hide, there can be good reasons why you may want to hide your identity or location when online. It can provide peace of mind for those who are worried about online security, and for many political dissidents, whistle-blowers and those with personal problems, it is essential.

It has become easier for organisations to identify individuals online and to track their communications. Traffic analysis techniques can reveal who is talking to whom, how often and when, simply by monitoring the network traffic that flows between systems.

Encrypting traffic doesn't prevent traffic analysis, because although individual emails and chat sessions cannot be read, the network traffic contains clearly readable headers that give the source and destination addresses of all packets. Routers and servers have to be able to read this, which means monitoring software can also read them. Using statistical analysis methods, it's then possible to see who's talking to whom, and to infer the nature of the conversation, if not its actual content.

This can have a huge impact on the unsuspecting online shopper, among others. E-commerce sites with price-discrimination policies often charge different amounts for products, depending on which country buyers are visiting from.

In some societies, expressing certain beliefs can be dangerous. Even in politically tolerant countries people may prefer to discuss taboo subjects anonymously. Victims of sexual crimes or those with embarrassing diseases may prefer not to announce their identities to the world at large.

In some cases, people exposing scandals in government and industry circles will talk to journalists only if they can guarantee anonymity. If a paper trail leads back to individual email addresses, the repercussions can be serious, even in the light of legislation to protect legitimate whistle-blowing.

TOR OF DUTY

Those with a genuine need for online anonymity have a number of possible methods at their disposal. One is the Tor network. Originally funded by the US Navy Research Lab before the Electronic Frontier Foundation (EFF) took it over in 2004, Tor can be the answer to many online anonymity problems.

Tor is a distributed system known as an onion router system. Like an onion, it has many layers. In this case, the layers automatically encrypt and tunnel communications through random paths, called virtual circuits, across the Tor network. Packets emerge from the network at a random point and continue on their journey with an IP address that bears no relation to the user's. Nothing can link you with the destination server.

For extra protection, and to reduce the overheads associated with building temporary virtual circuits, machines on the Tor network know only about which other servers have passed local traffic to them, and nothing about its overall path, its original source or final destination. For reasons of efficiency, after a timeout period of around a minute, the virtual circuit you were using collapses anyway. When traffic resumes, the Tor network seamlessly sets up another tunnel.

Even if a snooper compromises a Tor server, the machine can give away nothing more useful than the fact that encrypted traffic is flowing over specific ports. An attacker would have to compromise the exact entry point to the network and the correct exit point, and then match the time and number of packets entering and leaving the network to match the source with the destination. As the traffic emerges at random, this would be no mean feat. One question remains, though: where do these Tor servers come from?

Users who install the Tor software on their machines can use the network simply as a client, but they can also allow their machines to form part of the network itself. It's a little like a peer-to-peer file sharing network. Some people install the software and enable themselves as servers as a sign of their commitment to freedom of speech, while others may have a specific need to use the network as a client.

There's no pressure to allow your system to become a server, but the more servers that exist the more traffic the network can handle. Tor sounds perfect for those who need privacy, but there's something important to remember before we move on and show it in action.

After installation, Tor doesn't immediately anonymise all traffic that leaves your machine. It can protect traffic only from applications that are configured to route their traffic through an entry point to the network. Because most people use a web browser, the Tor website recommends you use Firefox as a Tor-aware browser with the Torbutton extension

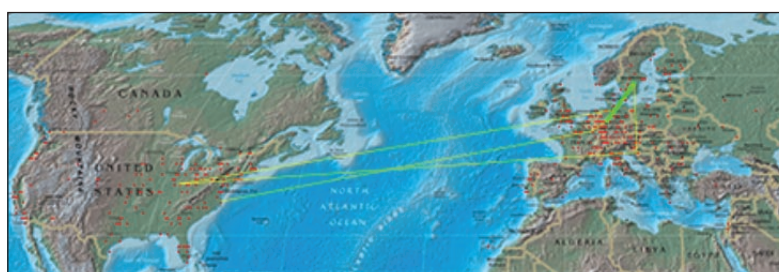
INTRODUCTION

The internet is enormous and complicated, so you might assume that using it anonymously would be both possible and fairly easy. However, whether you are sending an email, browsing a website or using internet messaging, everything you do is logged and can be traced back to you. Here we investigate an anonymising system that aims to preserve your privacy online.

Jon Thompson
IT Correspondent



contributors@computershopper.co.uk



◀ Data can take a convoluted path over the Tor network, as shown by the network map option

Don't follow the script Stopping JavaScript in your browser

The Tor team suggests a few other steps you can take to remain as anonymous as possible while online. JavaScript embedded within a webpage you browse to can collect information about your machine, even if you connect over the Tor network. To prevent this, you can install NoScript from the Firefox plug-ins site at <https://addons.mozilla.org/en-US/firefox/addon/722>.

NoScript simply refuses to allow any JavaScript to run in your browser unless you specifically allow it to do so. Click the NoScript logo in the bottom-right of Firefox's window and it provides options for controlling which sites can run scripts when you load their pages. The default setting for each page you load is that no script will run unless you explicitly authorise it.

installed. This will automatically route all web traffic over the Tor network when enabled.

INSTALLATION/CONFIGURATION

Installation is as simple as double-clicking the downloaded executable, which is available from the Tor site (<http://tor.eff.org>), and accepting the default settings. The Tor installation package also contains the Privoxy web privacy proxy, which is useful for blocking tracking cookies and adverts and for preventing third parties finding out too much about you and your system. It also contains the Vidalia graphical front-end to the Tor software.

Once you have installed everything, you probably won't notice much difference, but the Tor software and the Vidalia interface are running in the background. The Tor onion logo and the blue Privoxy 'P' logo appear in the taskbar. Right-click on the green Tor logo and you'll see a set of options that bring up various parts of the Vidalia interface.

The first is used to stop and start Tor. Next comes a useful bandwidth monitor, which gives a scrolling graphical indication of the traffic sent to and received from the Tor network. Note that this graph shows only Tor traffic.

If you have any problems, the next option may prove useful in solving them. The message log contains information about virtual circuits as they tunnel through the Tor network and then collapse. Related to this is the Network Map option. This graphical tool enables you to see the virtual circuits established from your machine. This information is encrypted and fed back along the tunnel, one anonymous step at a time. The Network Map shows the currently available Tor servers on the left, while a view of the world at the top of the screen shows the path your data takes. You can zoom this map for a better view.

Next is the New Identity option. Selecting this will collapse your existing virtual circuit through the Tor network. When you next connect to a remote server, the circuit creation process starts again using a completely different route around the network. Once you select this option, it becomes grey until you establish another virtual circuit by browsing the web.

The Control Panel option gives you the same options as we've covered so far, but also lets you set up your installation to become a Tor server. Click on the 'Setup Relaying' icon and the Tor configuration dialog will pop up. Basically, if you want to become part of the Tor network, click on the 'Relay traffic for the Tor network' tick box and press the Save button.

There are one or two other Tor configuration categories that are worth knowing about. The General category enables you to run Tor on system startup. The Appearance category lets you change the language and graphical style used by the interface. The advanced option

allows you to start Tor as a service rather than an application and set the Tor control port, used to ferry encrypted circuit information back to your machine. If you make any changes, save the configuration by pressing Save before exiting.

The next task is to install Torbutton on Firefox. Internet Explorer users shouldn't despair, as moving to Firefox is easy. At installation time, Firefox reads your bookmarks and will import them on demand. When you need anonymity, simply use Firefox rather than Internet Explorer.

To install Torbutton in Firefox, browse to <https://addons.mozilla.org/en-US/firefox/addon/2275> and click the 'Install Now' button. A pop-up appears, asking you to confirm the installation, after which the words 'Tor Enabled' appear in green at the bottom of the Firefox window whenever you use Tor to route your web traffic. Right-clicking this text and selecting the 'Toggle Tor Status' option alternates between using and not using Tor to route your traffic.

Interestingly, the Privoxy web privacy proxy that was installed when you installed Tor inserts itself automatically into the chain of network traffic whenever you enable Tor in Firefox. The proxy itself isn't particularly sophisticated and simply blocks traffic going to a wide range of tracking sites, according to a comprehensive set of patterns. Such sites work by embedding calls to their own servers in the webpages you visit. For example, a company might use a tracking service to read a cookie on your machine, which has recorded details of other sites you have visited. Privoxy simply stops this traffic. When Privoxy blocks adverts, it displays the URL of the advert in its place. It also displays hyperlinks so



▲ The Tor Detector page provides proof that Tor is successfully concealing your identity

you can see why the site was blocked, and to allow you to click through to the advertiser's site if you wish.

NO ID CHECKS

How do you know Tor is working, other than the assertion that it's been enabled in Firefox? The Tor Detector is the solution. Simply turn off Tor and browse to <http://check.torproject.org>. The site will show your IP address, which you may be able to check by opening a command line and entering the ipconfig command to see the public IP address your ISP gave you when you started your broadband connection. If you use a broadband router, this last step won't work.

Now enable Tor and refresh the webpage. The IP address that the site displays is that of a random node somewhere on the Tor network. Select the New Identity option by right-clicking the Tor logo in the taskbar and refresh the page again. The new IP address reflects the fact that your virtual circuit was torn down and rebuilt.

With Tor enabled, right-click on the blue Privoxy icon on the taskbar and select 'Show Proxy Window'. The log file shows the web objects it has processed. Some have the word 'crunch!' after them in bold letters to indicate objects the proxy has filtered out. You'll also see places on some webpages where Privoxy has put a URL instead of blocked content.

Because of the extra hops your traffic takes through the Tor network, it's slower than connecting to websites directly. For those with real privacy issues, however, this is a small price to pay, and the more servers that join the network the faster it will become. ☑

Free Tor Anonymity on Linux

Tor is available for Linux, too. The interface and operation are the same as those in Windows, but installation is a little more complicated. While you can build the software from the source archive, another option is to install the built packages. Using Ubuntu Linux, for instance, run the following commands:

```
# sudo gedit /etc/apt/sources.list
```

Add the following two lines to the file. These tell the apt-get software where to look for the packages.

```
deb http://mirror.noreply.org/pub/tor feisty main
deb-src http://mirror.noreply.org/pub/tor feisty main
```

Save the file and exit gedit.

Now type:

```
# sudo apt-get update
```

If apt-get says you're missing a public key to access the noreply.org site, you need to use the gpg command to add one, as follows:

```
# sudo gpg --keyserver subkeys.gpg.net --recv 94C09C7F
# sudo gpg --fingerprint 94C09C7F
# sudo gpg --export 94C09C7F | sudo apt-key add -
```

All being well, update the list of available packages and install Tor with the following:

```
# sudo apt-get update
# sudo apt-get install tor
```

Tor should start automatically.